

What Is Claimed Is:

1 1. A method for establishing a cryptographic key between a first node
2 and a second node, comprising:

3 sending a first message from the first node to the second node, wherein the
4 first message requests establishing the cryptographic key;

5 sending a second message from the second node to a key distribution
6 center, wherein the second message includes a first node identifier for the first
7 node, a second node identifier for the second node, and a message authentication
8 code created using a second node key belonging to the second node;

9 recreating the second node key at the key distribution center, wherein the
10 second node key was previously created using the second node identifier and a
11 secret key known only to the key distribution center;

12 verifying at the key distribution center the message authentication code in
13 the second message using the second node key; and

14 if the message authentication code is verified,

15 creating the cryptographic key at the key distribution center,

16 and

17 communicating the cryptographic key to the second node

18 and the first node.

1 2. The method of claim 1, wherein communicating the cryptographic
2 key to the second node and the first node includes:

3 encrypting a hash value and the cryptographic key using the second node
4 key to create a first encrypted key;

5 recreating a first node key belonging to the first node, wherein the first
6 node key was previously created using the secret key and the first node identifier;

7 encrypting the hash value and the cryptographic key using the first node
8 key to create a second encrypted key;
9 sending a third message from the key distribution center to the second
10 node, wherein the third message includes the first encrypted key and the second
11 encrypted key;
12 decrypting at the second node the first encrypted key from the third
13 message to recover the hash value and the cryptographic key;
14 verifying the hash value at the second node; and
15 if the hash value is verified,
16 sending a fourth message to the first node from the second
17 node, wherein the fourth message includes the second encrypted
18 key and a key confirmation value so that the first node can confirm
19 that the cryptographic key has been established,
20 decrypting at the first node the second encrypted key from
21 the fourth message to recover the hash value and the cryptographic
22 key,
23 verifying the hash value at the second node,
24 establishing at the first node that the second node has the
25 cryptographic key, and
26 if the hash value is verified and it is established at the first
27 node that the second node has the cryptographic key,
28 sending a fifth message to the second node
29 from the first node so that the second node can
30 confirm that the cryptographic key has been
31 established.

1 3. The method of claim 2, wherein the first message includes the first
2 node identifier, the second node identifier, a third identifier for the key
3 distribution center, and a first nonce, wherein a nonce is a random number
4 selected for message confirmation purposes that has a statistically low probability
5 of being reused.

1 4. The method of claim 3, wherein the second message includes the
2 third identifier, the second node identifier, the first node identifier, a second
3 nonce, the first nonce, and the message authentication code, wherein the message
4 authentication code is created from the third identifier, the second node identifier,
5 the first node identifier, the second nonce, and the first nonce.

1 5. The method of claim 4, wherein verifying the message
2 authentication code includes:
3 creating a test message authentication code from the third identifier, the
4 second node identifier, the first node identifier, the second nonce, and the first
5 nonce using the second node key; and
6 comparing the test message authentication code with the message
7 authentication code.

1 6. The method of claim 5, wherein the hash value is created from the
2 second node identifier, the first node identifier, the second nonce, and the first
3 nonce.

1 7. The method of claim 6, wherein the third message includes the
2 second node identifier, the first node identifier, the second encrypted key, and the
3 first encrypted key.

1 the second node identifier, the first node identifier, and a second
2 confirmation value.

1 14. The method of claim 13, wherein creating the second confirmation
2 value at the first node includes:
3 reordering the first nonce and the second nonce recovered by decrypting
4 the first confirmation value to create the second confirmation value; and
5 encrypting the second confirmation value using the cryptographic key.

1 15. The method of claim 14, wherein confirming at the second node
2 that the cryptographic key has been established includes:
3 decrypting the second confirmation value using the cryptographic key; and
4 verifying that the second nonce was sent in the second message.

1 16. The method of claim 1, further comprising:
2 creating the second node key, wherein the second node key is created
3 using the secret key and the second node identifier; and
4 installing the second node key into the second node prior to deployment of
5 the second node.

1 17. The method of claim 2, further comprising:
2 creating the first node key, wherein the first node key is created using the
3 secret key and the first node identifier; and
4 installing the first node key into the first node prior to deployment of the
5 first node.

1 18. A computer-readable storage medium storing instructions that
2 when executed by a computer cause the computer to perform a method for
3 establishing a cryptographic key between a first node and a second node, the
4 method comprising:
5 sending a first message from the first node to the second node, wherein the
6 first message requests establishing the cryptographic key;
7 sending a second message from the second node to a key distribution
8 center, wherein the second message includes a first node identifier for the first
9 node, a second node identifier for the second node, and a message authentication
10 code created using a second node key belonging to the second node;
11 recreating the second node key at the key distribution center, wherein the
12 second node key was previously created using the second node identifier and a
13 secret key known only to the key distribution center;
14 verifying at the key distribution center the message authentication code in
15 the second message using the second node key; and
16 if the message authentication code is verified,
17 creating the cryptographic key at the key distribution center,
18 and
19 communicating the cryptographic key to the second node
20 and the first node.

1 19. The computer-readable storage medium of claim 18,
2 wherein communicating the cryptographic key to the second node and the first
3 node includes:
4 encrypting a hash value and the cryptographic key using the second node
5 key to create a first encrypted key;

4 the key recreating mechanism that is further configured to recreate a first
5 node key belonging to the first node, wherein the first node key was previously
6 created using the secret key and the first node identifier;
7 the encrypting mechanism that is further configured to encrypt the hash
8 value and the cryptographic key using the first node key to create a second
9 encrypted key;
10 a third sending mechanism that is configured to send a third message from
11 the key distribution center to the second node, wherein the third message includes
12 the first encrypted key and the second encrypted key;
13 a first decrypting mechanism at the second node that is configured to
14 decrypt the first encrypted key from the third message to recover the hash value
15 and the cryptographic key;
16 a second verifying mechanism that is configured to verify the hash value at
17 the second node; and
18 the second sending mechanism that is further configured to send a fourth
19 message to the first node from the second node, wherein the fourth message
20 includes the second encrypted key,
21 a second decrypting mechanism at the first node that is configured to
22 decrypt the second encrypted key from the fourth message to recover the hash
23 value and the cryptographic key,
24 a third verifying mechanism that is configured to verify the hash value at
25 the second node,
26 an establishing mechanism at the first node that is configured to establish
27 that the second node has the cryptographic key, and
28 the first sending mechanism that is further configured to send a fifth
29 message to the second node from the first node so that the second node can
30 confirm that the cryptographic key has been established.